UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,155	11/03/2003	Massimiliano Antonio Poletto	RIV-0550	5551

87555 7590 03/17/2010

Riverbed Technology Inc. - PVF
c/o Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618

EXAMINER	
BARQADLE, YASIN M	

ART UNIT	PAPER NUMBER
2456	

MAIL DATE	DELIVERY MODE
03/17/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/701,155	POLETTO ET AL.	
	Examiner	Art Unit	
	YASIN BARQADLE	2456	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

2. The amendment filed on November 19, 2009 has been fully considered but are moot in view of the new grounds of rejection.

Note: Applicant's Terminal Disclaimer has not been approved because a POA SIGNED ON BEHALF OF THE ASSIGNEE MUST BE ACCOMPANIED BY A 373(B) STATEMENT. PLEASE HAVE A NEW TD FILED WITH THE 373(B) STATEMENT.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In*

re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-17 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-22 of copending Application No. 10701154 and claims 1-36 of copending Application No. 10701356. Although the conflicting claims are not identical, they are not patentably distinct from each other a comparison between instant application independent claim 1 and the claims 1 and 14 (of the copending application number 10701154) and claims 1, 19, and 25 (of the copending application number 10701356) reveal the copending claims are simply species of the broader claim 1 of the instant application. Hence, claim 1 of the instant

application is generic to the species of the invention covered by independent claims of the copending applications stated above. Thus, the broad generic invention is anticipated by the narrower species of the co-pending invention, thus without a terminal disclaimer, the species claims preclude issuance of the generic application. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993).

Instant Application **10/701155**	Copending Application **10/701154**	Copending Application **10/701356**
Claim 1: A memory device storing a data structure for tracking network behavior, comprising:	Claims 1: A system, comprising: a plurality of collector devices that are disposed to collect statistical information on packets that are sent between nodes on a network;	Claims 1: A device comprising:
a connection table that maps each node of a network to a record **object that stores information about traffic to or from the node** and between that node and others nodes in the network.	**an aggregator that receives network data from the plurality of collector devices,** and **which produces a connection table that maps each node on the network to a record that stores information about traffic to or from the node.**	a processor; a memory storing **a connection table that maps each node of a network to** a host **object, the connection table stores information about traffic to or from the node.**
	Claim 14, A method,	Claim 19, A computer

1	comprises: providing a plurality of collector devices in a network to collect statistical information on packets that are sent between nodes on a network; and sending statistical information from the collector devices to an aggregator, the aggregator --- **producing a connection table that maps each node on the network to a record that stores information about traffic to or from the node** 1 and 14	program product residing on a computer readable medium for use in detecting network intrusions comprises instructions for causing a processor to: --- store a **connection table that maps each node of a network** to a host **object, the connection table stores information about traffic to or from the node** 1, 19 and 25
2	8 and 17	5
3	9 and 18	6
4	10 and 19	7
5	11 and 20	8
6	12 and 21	9 and 30
7 and 8	13 and 22	10 and 31

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1–9 and 11-17-23 and 25-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tams et al U.S. Publication Number (20030069952), hereinafter " Tams" in view OFFICIAL NOTICE.

As per claim 1, Tams (20030069952) teaches a computer system (fig. 2, 162 and fig. 9) for tracking network behavior (¶ 0079-0081 and ¶0198), comprising:

a processor and storage device storing a connection table (fig, 2, data table and Table 2, page 11. See also fig. 9) that maps each node of a network (host A-host B) to a record that stores information about traffic to or from the node and between that node and other nodes in the network (number of packets in fig. 9 for example) (¶ 0157-0164 and ¶0210. See TABLE 2, page 11).

Tams teach the claimed invention substantially as discussed above

Tams do not explicitly teach records including information indicating whether a node is operating as a client or a server.

OFFICIAL NOTICE is taken that network information indicating whether a node is operating as a client or a server is well known in the art.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to identify a node operating as a server or a client based on for example a port numbers used. A packet indicating a traffic from well know port 25 is identified as a mail server and a packet indicating a traffic from well know port 80 can be identified as an HTTP packet from a web server.

As per claims 2 and 3, Tams teaches wherein the connection table includes a plurality of records that are indexed by source and destination address (See TABLE 2, page 11 and 0021 and ¶0178).
As per claim 4, Tams teaches the device of claim 1 wherein the connection table includes a plurality of records that are indexed by time (¶0198 and ¶0201-0206; see steps in fig. 8).

As per claim 4, Tams teaches the computer system of claim 1 wherein the connection table includes a plurality of records that are indexed by time (¶0198 and ¶0201-0206; see steps in fig. 8).

As per claim 5, Tams teaches the computer system of claim 1 wherein the connection table includes a plurality of records, that are record objects, which are indexed by source address, destination address and time (See TABLE 2, page 11 and ¶ 0198 and ¶ 0201-0206. See also fig. 9 ¶ 0201 and ¶ 0178).

As per claim 6, Tams teaches the computer system of claim 1 wherein the connection table is a plurality of connection sub-tables each sub-table having data pertaining to network traffic over different time scales (¶0198 and ¶0201-0208; see the time scale data structure (709,711,713 and 715 in fig. 7).

As per claim 7, Tams teaches the computer system of claim 6 wherein the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table. (¶0198 and ¶0201-0208; see the time scale data structure (709,711,713 and 715 in fig. 7).

As per claim 8, Tams teaches the device of claim 7 wherein the at one sub-table holds records received from all collectors over the time scale of the table (¶0198 and ¶0212).

As per claim 9, Tams teaches the computer system of claim 5 wherein the addresses indexing the connection table are IP addresses (See TABLE 2, page 11).

As per claim 11, Tams teaches the computer system of claim 1 wherein the host record of a first host maps that firs host (host A, figure 9) to a second host (host B and host C) which communicates with the first host to a "host pair

record" that has information about all the traffic from between the first and second hosts (Fig. 9 and 10; ¶0201 and ¶0209-0210).

As per claim 12, Tams shows a connection table includes a two level mapping that enables a consuming computer system to obtain summary information about one host for a first level mapping and about the traffic between any pair of hosts in either direction, between a first one of the hosts of any pair to a second one of the hosts of the any pair and from the second one of the host of the any pair to the first one of the host for the any pair for a second level mapping (figure 9-10 and ¶0201-0209).

As per claim 13, Tams teaches the computer system of claim 1 wherein a record the connection table comprises a plurality of host record, a host record stores a measure of the number of bytes, packets, and connections that occurred between hosts during a given time-period (¶ 0157-0164 and ¶0210. See TABLE 2 and figures 9 and 10).

As per claim 14, Tams teaches wherein data in the record is organized by well known transport protocols and well-known application-level protocols (¶ 0151-0157 and ¶0161-168. See TABLE 2 and TABLE 4A-4B and figures 9-10).

As per claim 15, Tams teaches the computer system of claim 13 wherein host

records have no specific memory limit (¶0202-0206).

As per claim 16, Tams teaches the computer system of claim 1 wherein for application-level protocols and for every pair of hosts, the connection table stores statistics for traffic between the hosts (¶ 0151-0157 and ¶0161-168. See TABLE 2 and TABLE 4A and 4C in page 11).

As per claim 17, Tams teaches the computer system of claim 16 wherein the connection table stores protocol-specific records as (protocol, count) key-value pairs (¶ 0151-0157 and ¶0161-168. See TABLE 2 and TABLE 4A-4B in page 11).

As per claim 18, Tams teaches a memory computer system storing a data structure for tracking network behavior (fig. 7, 707), the data structure comprising:

a processor; and a storage device storing a connection table (table 2 and fig. 9, 920) that maps each node of a network to a record that stores connection information about traffic to or from the node and between that node and others nodes (host A-host B or Host A-host E (fig. 9) that have connections with the node in the network (¶02090, the connection table indexed according to at least a first one of source address, destination address and time (¶0021 and ¶0178); the connection table further including in the records fields for storing

statistical information for traffic between the hosts (packet counts in table 2 or fig. 9).

As per claim 19, Tams teaches the computer system of claim 1 wherein the plurality of records are record objects (See TABLE 2, page 11 and ¶ 0198 and ¶ 0201-0206. See also fig. 9 ¶ 0201 and ¶ 0178).

As per claim 20, Tams teaches the computer system of claim 18 wherein the connection table is a second plurality of connection sub-tables, each sub-table having data pertaining to network traffic over different ones of corresponding second plurality of time scales (fig. 7, 207 and figures 9-10).

As per claim 21, Tams teaches the computer system of claim 18 wherein the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table (See fig. 7 and fig. 9).

As per claim 22, Tams teaches the computer system of claim 18 wherein the at one sub-table holds records received from all collectors in the network over the time scale of the table (See fig. 7 and fig. 9).

As per claim 23, Tams teaches the computer system of claim 18 wherein the addresses indexing the connection table are IP addresses (¶0021 and ¶0178).

As per claims 25-27, these claims correspond to claims 11-14, therefore they are rejected with the same rational.

As per claims 29-30, these claims correspond to claims 16-17, therefore they are rejected with the same rational.

Claims 10 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tams et al U.S. Publication Number (20030069952), hereinafter " Tams" in view of Maufer et al U.S. Patent Number (7120930), hereinafter " Maufer".

As per claims 10 and 24, although Tams shows substantial features of the claimed invention including a table with plurality of records, he does not explicitly show a physical [layer] address to IP address map that is used to determine Host ID.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system disclosed by Tams, as evidenced by Maufer U.S. Patent Number (7120930).

In analogous art, Maufer whose invention is about a Method and apparatus for enhanced security for communication over a network including a mapping table accessible by a gateway computer used to form associations between a local address for the client and a destination address for a peer and a Security Parameters Index associated with IPSec-protected traffic from the peer (abstract), discloses a physical [layer] address to IP address map that is used to determine Host ID (col. 16, line 51-65 and table 300, fig. 5A. See also col. 5, lines 36-60).

Giving the teaching of Maufer, a person of ordinary skill in the art would have readily recognized the advantage of modifying Tams by employing the enhanced network security system of Maufer for particularly identifying traffic flowing from a remote address to the local address using physical layer (MAC) address to IP address mapping in order to verify hosts belonging to the private network from unknown intruders of the public network. In this way fake packets belonging to unknown sources are recognized and discarded.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yasin Barqadle whose telephone number is 571-272-3947. The examiner can normally be reached on 9:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dharia Rupal can be reached on 571-272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Yasin M Barqadle/
Primary Examiner, Art Unit 2456